Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

)
In the Matter of)
)
Facilitating Opportunities for Flexible, Efficient) ET Docket No 03-108
And Reliable Spectrum Use Employing Cognitive)
Radio Technologies)
)

PETITION FOR CLARIFICATION, OR IN THE ALTERNATIVE, RECONSIDERATION

I. INTRODUCTION

Cisco Systems, Inc. ("Cisco") hereby respectfully submits this Petition for Clarification, or in the Alternative, Reconsideration in the above-captioned proceeding.[1] Cisco largely supports the Commission's decision in this docket. This petition seeks clarification or modification of only two issues. First, the Commission's decision in this proceeding broadens the definition of software defined radios (SDRs) to include both operating parameters and "the circumstances under which a transmitter operates in accordance with Commission rules," such as dynamic frequency selection

[1] *Facilitating Opportunities for Flexible, Efficient and Radio Spectrum Use Employing Cognitive Radio Technologies*, ET Docket No. 03-108, Report and Order, released March 11, 2005 (hereinafter "Order").

(DFS) required for certain bands at 5 GHz for license-exempt devices.[2] The definition states that if the radio "can" be altered by making a change only in software, then it falls within the SDR definition.[3] While the text of the order indicates that radios "not designed or expected to be modified by a party other than the manufacturer," do not require SDR certification, this qualification is not included in the definition or otherwise clearly reflected in the rules.[4] Cisco's concern is that while many devices "can" be altered by software and therefore fall within the SDR definition, devices are often designed in a way that does not facilitate software changes because the manufacturer intends no future software changes, and does not intend others to make software changes. Cisco requests either clarification of the rules to specify the exclusionary class.

Secondly, Cisco is concerned that the security measures required by the Order that prevent unauthorized modifications by end users are potentially at odds with open source software licensing requirements upon which some of Cisco's equipment relies. To the extent manufacturers employ open source code in software, there exist contractual licensing obligations to make public software modifications to that code. As a result, there is arguably a potential issue that security measures grounded in open source

[2] Order at paras. 40, 47 and new rule Section 2.1(c), *to be codified at* 47 C.F.R. §2.1(c).

[3] *Id.*

[4] Id. at para. 51.

software must be disclosed. This requirement appears at odds with the Commission's intent, as indicated in its decision to provide confidential treatment of manufacturer filings of security measures. With the Commission seeking to broaden the opportunities for SDR certification, it would be helpful to open source manufacturers if the Commission could include in the text of an order a policy statement that software supporting such security measures must not intentionally be made public if doing so would reasonably increase the risk that security measures could be breached so that the radio could be operated in a manner inconsistent with U.S. rules. Such an expression of federal policy can help to guide open source manufacturers in the future, and can be a useful point of reference if disputes arise.

II. BACKGROUND

The Commission's Cognitive Radio docket provided a useful forum for the Commission to identify current developments in cognitive radio technology, and to adjust its equipment certification rules to ensure that its processing rules are clear and facilitate such technology. The docket represents an extension and expansion of the Commission's earlier decision on software-defined radios, recognizing that software is increasingly able to both define operating parameters of transmitters, as well as comply with other conditions that might be placed on the operations of transmitters, such as when they share a band with other types of devices. Cisco strongly supports the Commission's efforts to promptly adjust its rules to reflect these technological developments, and to ensure that, once SDR approval is obtained, further changes to radios via software changes are "permissive changes" that do not require re-certification of the device. Cisco has submitted its first SDR application, and looks forward to taking advantage of SDR rules in the future.[5]

Among the rule changes implemented by the Order are: (1) expanding the definition of SDR to include transmitters where software governs not just the operating parameters of the radio, but also the circumstances under which the radio transmits; (2) requiring security mechanisms to prevent software tampering that would allow a radio to transmit in a manner inconsistent with U.S. rules; (3) eliminating the requirement to submit software to the Commission, in favor of a requirement that the manufacturer describe how the software and security operates; and (4) permitting unlicensed "master" devices to be manufactured for world markets, provided that radios located in the U.S. are governed by software that ensures that they operate pursuant to U.S. rules. Cisco supports these improvements in the rules, but at the same time urges the Commission to clarify or reconsider two issues to better align the rules with its expressed intentions of the Commission, as stated in the text of the Order.

[5] Application of Cisco Systems, Inc. for certification of SDR radio module, Application No. LDK102056, filed May 24, 2005.

III. RULES SHOULD BETTER REFLECT EXCLUDED CLASS OF TRANSMITTING DEVICES

The Commission's rule defines software defined radios as follows:

> A radio that includes a transmitter in which the operating parameters of frequency range, modulation type or maximum output power (either radiated or conducted), or the circumstances under which the transmitter operates in accordance with Commission rules, can be altered by making a change in software without making any changes to hardware components that affect the radio frequency emissions.[6]
> (emphasis supplied)

As a result, a literal reading of the rule section 2.1(c) appears to sweep within its definition most devices that will be certified under the new rules adopted for 5250-5350 MHz and 5450-5750 MHz. which will need to employ Dynamic Frequency Control to avoid radars.[7] The only limitation contained within the definition, exempting some devices from SDR treatment, goes to devices that require both hardware and software changes to adjust "operating parameters" or "circumstances."

This definition appears to be directly at odds with the intent of the Commission, as expressed in the text of the Order, which states that the Commission expects "no change[s]" to the equipment certification process for

[6] Order at Appendix A, Section 2.1(c) of the Commission's rules.

[7] Revision of Parts 2 and 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) devices in the 5 GHz band, *Report and Order*, ET Docket No. 03-122, 18 FCC Rcd 24484 (2003).

the “vast majority” of WiFi devices.[8] “[R]adios that are not designed or expected to be modified by a party other than the manufacturer…” are not intended to be treated as SDRs.[9] However, the definition contained in the rule part does not reflect the limitation or exclusion articulated in the text.

The new rules appear to try to compensate for this omission by including, in a reformulated section 2.944, a subsection b which provides that “[a]ny radio in which the software is designed or expected to be modified by a party other than the manufacturer and would affect the operating parameters… or circumstances under which the transmitter operates…” must be certified as a software defined radio. However, the affirmative statement in section 2.944(b) is not the simple inverse of the negative statement printed in the text, for two reasons. First, the definition in section 2.1(c) controls what is or is not a software defined radio. To the extent the definition fails to reflect the Commission’s intent to exclude certain radios, the damage has already been done in the definition. Second, section 2.944(b) provides a statement that if the manufacturer intends to have modifications to the device performed by another party, then the device “must” be certified as an SDR. In short, this provision appears to simply underscore that the SDR certification applies in a specific factual case, e.g., when the manufacturer intends to have others modify the software. The section 2.944(b) rule language does not on its face appear to alter the more

[8] Order at para. 51.

[9] Id.

fundamental definition or exclude any radio from the SDR certification process. And, while it is possible to infer the inverse proposition from the rule (that if there is no design for or expectation of modification, then SDR does not apply), that inference appears to be inapposite to the SDR definition which contains no such limitation.

In Cisco's case, we expect to produce radios:

- whose "operating parameters" or "circumstances" are defined by software that is pre-set at the factory;
- that are not designed or intended to be modified by others; and
- that Cisco does not intend to modify after the device leaves the factory.[10]

Because the transmitters are controlled by software that "can" in some absolute sense modify the radio, the rules as written appear to suggest that an SDR certificate is required in such cases. However, the text of the order appears to suggest that the Commission did not intend such a result.

> "Only a relatively small number of radios will be affected…because most RF affecting radio software is not designed or expected to be modified…" by others "…and we are not changing the rules for radios that are not designed or expected to be modified…" by others. "Thus, there will be no change to the authorization requirement for the vast majority of devices including … WiFi equipment, provided the software that directly or indirectly controls the RF emissions of these devices is not designed or expected to be modified by…" others.[11]

[11] Order at para. 51.

Reading from the text, it appears that the Commission intended to establish a broad excluded "class." Where the manufacturer does not intend and enable others to modify software, no SDR certification is required, even if the device "can" be modified by a software change, such as by the manufacturer itself.

In Cisco's view, the Commission needs to sort out the ambiguity presented by the differences between the rule and the text of the order. The use of the verb "can" in the SDR definition, such that a radio is an SDR if its software "can" be modified, is overbroad. The issue is not whether a manufacturer "can" modify a radio by changing its software, but whether the manufacturer has designed or built the radio to enable such changes, and therefore expects to make such changes itself or expects others to make such changes. If not, then the radio should not be filed as an SDR. The public interest is better served if the Commission's SDR certification process is reserved for SDRs that are intended to be altered after manufacture and distribution, whether by the manufacturer or by parties other than the manufacturer, such as in the field by end users. SDR applications must contain new and additional information, such as software descriptions and security requirements, and are also subject to longer processing times because these must be reviewed by the FCC lab.[12] We respectfully request

[12] Cisco understands that the staff has announced a policy of requiring all new certifications for the new 5 GHz bands to be processed by the FCC lab until further notice. Cisco's objection to the SDR rules as adopted does not rest on "who" processes 5 GHz applications, but on the apparent ambiguity about when an SDR application must be filed.

that the Commission clarify, or alternatively, reconsider, its rule language to better reflect the text of the order, and specifically to exclude devices that are not designed or expected to be modified by the manufacturer or by other parties from its definition in section 2.1(c).

IV. CLARIFICATION TO MANUFACTURERS TO KEEP SECURITY MEASURES OUT OF THE PUBLIC DOMAIN IS NEEDED

The Commission correctly establishes security requirements intended to prevent unauthorized changes to SDRs that would enable others to modify their operations in a manner inconsistent with U.S. rules. Significantly, the Commission did not specify any particular security mechanism or technology, but mandated the outcome that it desired – software cannot be easily modifiable by end users.[13] This is critical to providing flexibility to manufacturers who are interested in certifying devices as SDRs, and allows security technology to continue to develop and improve. Cisco supports these decisions, as well as the consolidation of all SDR-related rules into a new section 2.944.

In addition, the Order eliminates the requirement to submit a copy of the source code itself for FCC examination, in favor of a requirement that allows an applicant to submit a high level software operational description or flow diagram, to include a description of how the security method will ensure

[13] Section 2.944(a).

that the radio can only be operated under U.S. rules.[14] The Order further provides that information about how a transmitter will comply with the security requirement is proprietary to the manufacture. The Order designates this information as proprietary because disclosure of such information could result in competitive harm and could assist unauthorized parties in determining ways to defeat the security measures. The Commission therefore modified its confidentiality rules to declare that the Commission will treat information about security measures as presumptively confidential should a Freedom of Information Act request be filed by another party.[15]

The discussion in the text presumes that the software embedded in the radios is fundamentally proprietary in nature. While we believe most radios do employ software that is proprietary, there are also radios that rely upon open source software. Open source software is associated with licensing requirements that compel the user to make public modifications to the open source code.

Cisco is concerned that the security measures required by the Order that prevent unauthorized modifications by end users are potentially at odds with open source software licensing requirements upon which some of Cisco's equipment relies. Due to the licensing requirements, there is arguably a potential issue that security measures that are based on open source software

[14] Order at paras. 67-68.

[15] Id. at para. 68.

must be disclosed. This requirement appears at odds with the Commission's strong preference, as indicated in its decision to provide confidential treatment of manufacturer filings of security measures, to keep security measures out of the public domain. With the Commission seeking to broaden the opportunities for SDR certification, it would be helpful to open source manufacturers if the Commission could include in the text of an order a policy statement that software supporting security measures for SDR must not intentionally be made public if doing so would reasonably increase the risk that security measures could be breached so that the radio could be operated in a manner inconsistent with U.S. rules.

In seeking this clarification, Cisco is not seeking in any way unilateral FCC modification to any open source licensing agreement. In fact, it is not completely clear given the relatively undeveloped state of the law whether the modifications that Cisco might make to open source software trigger the license provisions that require software modifications to be made public.[16] Cisco is merely seeking a policy statement that it is federal policy to keep security measures for SDRs out of the public domain. This expression of federal policy can help to guide open source manufacturers in the future, and can be a useful point of reference if disputes arise.

IV. CONCLUSION

[16] For example, it may make a difference whether changes are made to the kernel of a chipset, which may or may not be considered "software" under the open source agreements.

Cisco urges the Commission to adopt either a clarification of its Order, or an Order on Reconsideration, which further specifies the SDR definition and the need to keep security measures out of the public domain.

Respectfully submitted,

CISCO SYSTEMS, INC.

Mary L. Brown
Senior Telecommunications
Policy Counsel

1300 Pennsylvania Ave. NW
Suite 250
Washington, DC 20004
202.354.2923
mary.brown@cisco.com

June 3, 2005